OD/NIH/HHS
Administrative Policy & Procedure

Wireless Communication
(BlackBerry and Cellular Telephone Service)

Purpose

This document clarifies the policy and procedures for requesting, procuring, and managing the resources associated with wireless communication devices in the OD, i.e. Personal Digital Assistants (PDA) and cell phones. See NIH Policy and Procedure for Acquiring and Managing Personal Digital Assistants.

Background

Wireless communication devices, such as PDAs and cell phones, offer substantial potential benefit to OD. PDAs are palm-sized computing devices that give OD staff access to:
- locally stored information; and
- email, Internet and/or voice communication.

OD management must ensure that PDAs and cell phones procured for OD staff use are justified, effective, and managed appropriately.

Policy

This policy applies to all OD/NIH wireless communication devices and services for all uses (e.g., office, home, field locations, telecommuting sites).

The RIM BlackBerry is the HHS standard PDA device recommended for OD wireless email and voice communications.

If only voice communications are needed, OD cell phone managers can authorize cell phone acquisition/use per the OD/NIH Cell Phone Policy.

Justification for the acquisition and use of wireless communication devices
Requests for BlackBerry or cellular telephone devices/service must show how the device helps employees responsively and productively carry out job responsibilities. Examples include *providing:*
- a valuable back-up communication resource during network disruptions
- support and monitoring of projects that require attention after work hours
- access to staff who are routinely out of the office, e.g., attending meetings, providing technical assistance, telecommuting, or traveling.

Procedures

The procedures for acquiring OD/NIH-furnished PDAs are described below. See the OD/NIH Cell Phone Policy for cell phone procedures.

Write Justification for Wireless Communication Service Request

The requester must write a justification email that explains in detail how the availability of OD-furnished wireless communication equipment and/or service is essential to support OD's mission. The request must include the:

- Justification explaining the intended use of the wireless service, i.e. the reason the OD staff needs the wireless device.
- Name, office, telephone number, building, and room number of the OD staff.
- Type of wireless device requested.
- Time frame for use, e.g., indefinite, intermittent project work, etc.

Submit memo for approval

The OD Executive Officer (EO) must review and approve, as appropriate, the acquisition of all new PDAs and related service contracts for OD staff.

OD Office Directors can approve:
- Upgrades/replacements of BlackBerry devices;
- Renewals of BlackBerry service.

Order Wireless Communication Resources

The OD organization may order the wireless communication devices/service *only* after approval of the request.

Inventory and Property Management

PCO
Upon delivery and receipt of the wireless equipment, the Property Custodial Officer (PCO) in the authorized staff's organization will decal the equipment and enter the necessary information into the Property Management Information System (PMIS).

OD staff
Upon receipt, the OD staff must:
- password-protect PDAs. When password protecting the PDAs (BlackBerry model 6710

or later version) OD staff must enter:

- o their name, office, telephone number, building, and room number.
- o the text *"This is Federal property."*

Note: OIT desktop support staff will help OD staff per the password protection when setting up and supporting BlackBerry devices.

- ▪ Contact OIT via TASC@nih.gov (4-3278) to register the PDA and install client software.)

If the equipment at any time is lost or stolen, the authorized staff must:
- ▪ prepare the HHS Form 342-Report of Survey immediately
- ▪ submit the form to their PCO for further review.

If theft is suspected, the authorized staff must:
- ▪ report the incident immediately to the appropriate law enforcement authority.
  On campus - NIH Police. Off campus - the appropriate local authority.
- ▪ attach copies of any relevant police reports to the Report of Survey form. The complete package will be forwarded through the employee's supervisor to the PCO for investigation.

Sensitive Information

OD staff must not use PDAs to send or store sensitive information (e.g., proprietary data, records about individuals requiring protection under the Privacy Act, data not releasable under the Freedom of Information Act, data that, if disclosed or improperly used, could adversely affect NIH's ability to accomplish its mission, etc.)

Policy Exceptions

The OD EO and NIH CIO must approve all PDA exceptions (i.e. if procuring something other than the BlackBerry device). Exception requests must include documentation that supports the reason that a BlackBerry device cannot meet the OD's needs.